5 techniques commonly used by hackers when targeting the retail sector

The retail sector is becoming one of the top concerns of cybercriminals.

The rapid development of the retail sector as well as electronic payment and online payment activities has made it one of the top concerns of cybercriminals in the past few years.

According to a new study conducted by cybersecurity organization IntSights, retailers around the world have suffered more than $ 30 billion in losses due to simple to complex cyber attacks. is not taking into account many unreported cases or businesses not disclosing information to ensure brand reputation.

Please read along with TipsMake.com to take a look at 5 techniques commonly used by hackers to attack the retail sector below.

Credential stuffing

Credential stuffing is a hacking technique where hackers often use large amounts of login information (bought on the dark web or gathered from major security breaches). to hack into corresponding user accounts on online shopping websites, retailer websites and product purchases. The stolen account information usually includes a list of usernames, email addresses, and corresponding passwords.

According to statistics, more than 10 billion credential stuffing attacks have been launched by hackers towards global retail websites in 2019.

Near Field Communication (NFC)

Mobile phones, price scanners and card readers are easy targets for NFC-based attacks. Even malware can transfer the phone from an infected phone to the retail system when scanning a QR code. However, hackers will use many different methods to transfer data, such as using a third device to block the connection between the two original electronic devices. In addition, accessing the device opens up opportunities for hackers to obtain credit card information and other types of payment data.

RAM Scraping

RAM Scraping is the process of automatically collecting information from RAM. Hackers use this technique to gain access to point-of-sale (PoS) software. Each card transaction leaves data in the retailer's payment terminal (PoS payment device). Hackers will inject malware into PoS software and quickly collect data stored in PoS payment device before it disappears. It should be noted that the text strings containing credit card information may still be stored in the retailer's database for seconds, minutes or hours after payment is completed.

Magnetic reading device

The crooks are not always forced to break into the target system to gain login information. The magnetic strip of bar codes on credit and debit cards is what hackers take advantage of. They can easily glean data from a swipe, including card numbers and PINs. This information will continue to be used for malicious purposes or sold in large quantities for profit. In response to this attack technique, many card issuers have replaced magnetic strips with chips. The chip will generate a unique transaction code, which can only be used in one transaction.

Social engineering (Social Engineering)

This is an age-old attack technique, popular and never outdated. It is simply because it strikes human error, thereby breaking the normal security processes, accessing systems and networks to gain financial benefits. In simple terms, this is a scam technique. Hackers use social techniques to hide their true identities and motives with the appearance of a trusted source of information or personal identity. The goal is to influence, manipulate, or trick users into giving up privileged information or access in an organization. Besides, they can also create malicious websites, with the aim of fooling the gullible people access, providing personal information, thereby losing control of their data.

No system is absolutely secure. Above all, raise your awareness of network security to protect yourself. At the same time, organizations, businesses and service providers also need to be responsible for ensuring the security of their customers and systems.